ABSTRACT

A bit string obtained by sampling, every the number s, bits of a bit string whose output sequence is M sequence, when the bit number per one cycle of the M sequence is prime to the derived value, constitutes M sequence of a linear feedback shift register having other construction. Further, the linear feedback shift register can be determined from bits corresponding to at least two cycles by Berlekamp-Massay algorithm, whereby the linear feedback shift register 11 can be easily and dynamically reconstructed based on the initial state value.

530,574

(12)特許協力条約に基づいて公開された国際出願

Rec'd PCT/PTO 07 APR 2005

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年4 月15 日 (15.04.2004)

PCT

(10) 国際公開番号
WO 2004/032098 A1

(51) 国際特許分類[7]: G09C 1/00, G06F 7/58

(21) 国際出願番号: PCT/JP2003/008794

(22) 国際出願日: 2003 年7 月10 日 (10.07.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-294184 2002 年10 月7 日 (07.10.2002) JP

(71) 出願人 (米国を除く全ての指定国について): 小林 朗 (KOBAYASHI,Akira) [JP/JP]; 〒662-0894 兵庫県 西宮市 上ヶ原四番町４番３３−７０８ Hyogo (JP).

(71) 出願人 および
(72) 発明者: 森井 昌克 (MORII,Masakatsu) [JP/JP]; 〒770-0816 徳島県 徳島市 助任本町３−２６ Tokushima (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 白石 善明 (SHIRAISHI,Yoshiaki) [JP/JP]; 〒577-0027 大阪府 東大阪市 新家中町１−８−９０６ Osaka (JP).

(74) 代理人: 江藤 聡明 (ETOH,Toshiaki); 〒104-0031 東京都 中央区 京橋２丁目８番１８号 昭和ビル Tokyo (JP).

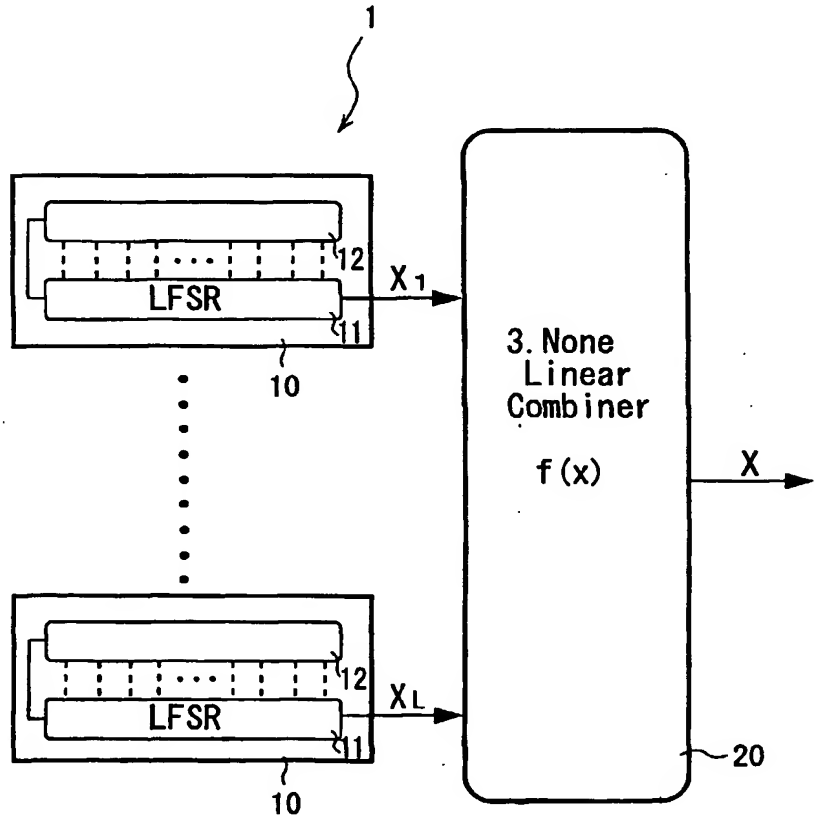
(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM,

[続葉有]

(54) Title: PSEUDO-RANDOM NUMBER GENERATION METHOD AND PSEUDO-RANDOM NUMBER GENERATOR

(54) 発明の名称: 疑似乱数発生方法及び疑似乱数発生器



(57) Abstract: A bit string sampled by s pieces from the M-series bit string of an output series becomes an M-series of a linear feedback shift register having another configuration when a bit count m of one cycle of the M-series is relatively prime to the obtained value s. Moreover, by using the Berlekamp-Massay algorithm, it is possible to obtain a linear feedback shift register minimum and equivalent from the bit string having the number of bits of at least two cycles. By utilizing this, it is possible to easily and dynamically modify the configuration of the linear feedback shift register (11) according to the initial value.

(57) 要約: 出力系列がM系列のビット列をs個ごとにサンプルしたビット列は、そのM系列の1周期分のビット数mと導出値sが互いに素であるときは、他の構成を有する線形フィードバックシフトレジスタのM系列になり、また、パートイキャンプマッセイアルゴリズムによって、少なくとも2周期分以上のビット数を有するビット列から最小で等価の線形フィードバックシフトレジスタを求めることができることを利用して、初期値に基づき線形フィードバックシフトレジスタ11の構成を容易かつ動的に変更する。

WO 2004/032098 A1